REMARKS

In the non-final Office Action, the Examiner rejects claims 1-3, 6, 9-13, 15-21, and 23-30 under 35 U.S.C. § 102(b) as anticipated by ISHIKAWA (U.S. Patent Application Publication No. 2001/0037314); and rejects claims 4, 5, 7, 8, 14, 22, and 31 under 35 U.S.C. § 103(a) as unpatentable over ISHIKAWA in view of WILLIAMS (U.S. Patent Application Publication No. 2001/0054029). Applicants respectfully traverse these rejections.[1]

By way of the present amendment, Applicants amend claims 22 and 31 to improve form. No new matter has been added by way of the present amendment. Claims 1-31 remain pending.

REJECTION UNDER 35 U.S.C. § 102(b) BASED ON ISHIKAWA

Claims 1-3, 6, 9-13, 15-21, and 23-30 stand rejected under 35 U.S.C. § 102(b) as allegedly anticipated by ISHIKAWA. Applicants respectfully traverse this rejection.

A proper rejection under 35 U.S.C. § 102 requires that a single reference teach every aspect of the claimed invention. Any feature not directly taught must be inherently present. See M.P.E.P. § 2131. ISHIKAWA does not disclose or suggest the combination of features recited in claims 1-3, 6, 9-13, 15-21, and 23-30.

For example, independent claim 1 is directed to a method for detecting spam. The method includes identifying normal users visiting a web site and determining an

[1] As Applicants' remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicants' silence as to assertions by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., whether a reference constitutes prior art, motivation to combine references, assertions as to dependent claims, etc.) is not a concession by Applicants that such assertions are accurate or such requirements have been met, and Applicants reserve the right to analyze and dispute such assertions/requirements in the future.

occurrence of spamming on the web site based at least in part on the identified normal users. ISHIKAWA does not disclose or suggest this combination of features.

For example, ISHIKAWA does not disclose or suggest determining an occurrence of spamming on a web site based at least in part on identified normal users visiting the web site. The Examiner relies on paragraphs 0016, 0017, and 0052 of ISHIKAWA as allegedly disclosing this feature (Office Action, p. 3). Applicants respectfully disagree with the Examiner's interpretation of ISHIKAWA.

At paragraph 0016, ISHIKAWA discloses:

> Upon receipt of the request for information from the user, the merchant compares the current user information to aspects of the confirmation code, namely, the user identification code generated dynamically at the time the advertising link was loaded onto the user's computer. If the current user information matches the previously generated user identification code, or the confirmation code can otherwise be verified, the entry is recorded in a logging database file for the advertiser associated with the advertising link. Once the information is recorded in the merchant's advertiser log, the entry is further passed to an accounting management system, which tracks the amount of remuneration owed to each advertiser. If the user identification code does not match the user information, or cannot otherwise be verified, the entry is recorded in a predefined database, such as, a spam system database and the advertiser is not paid for the click. Additionally, in some embodiments, the user is presented a `dead page` stating that the link was generated fraudulently.

This section of ISHIKAWA discloses comparing a dynamically generated user identification code to current user information to determine if a click is spam. This section of ISHIKAWA does not disclose or suggest determining an occurrence of spamming on a web site based at least in part on identified normal users visiting the web site, as recited in claim 1. At most, this section of ISHIKAWA could be said to disclose determining if a click is normal or spam. This section of ISHIKAWA in no way

discloses or suggests that the determination of whether a click is normal or spam is based at least in part on identified normal users visiting the web site, as would be required by claim 1 based on the Examiner's interpretation of ISHIKAWA.

At paragraph 0017, ISHIKAWA discloses:

> A feature of preferred embodiments of the invention includes the dynamic generation of a confirmation code that comprises data that expires. An advantage to this feature is that the merchant placing the advertisement can verify the validity of the click on the advertisement by determining whether the confirmation code has expired. A further advantage to this feature is that an expired confirmation code alerts the merchant to potentially fraudulent activity and discourage illegal spamming.

This section of ISHIKAWA discloses determining the validity of a click on an advertisement based on expiration of a confirmation code. This section of ISHIKAWA does not disclose or suggest determining an occurrence of spamming on a web site based at least in part on identified normal users visiting the web site, as recited in claim 1. ISHIKAWA's confirmation code in no way relates to identifying normal users visiting a web site.

At paragraph 0052, ISHIKAWA discloses:

> Once a comparison is made to determine the validity or authenticity of the request, the results are recorded in an appropriate database. If the encrypted advertiser's identification is not valid, that is, the user identification code does not match the known data, or is beyond an acceptable threshold tolerance, for example, a predetermined time period, the entry is recorded in a predefined database, such as, an invalid response or a spam system database 54. If the advertiser's identification is valid, the entry is recorded in a logging database file for the particular advertiser 56. Once the information is recorded in the advertiser's log, the entry is further passed to an accounting management system 58, which tracks the amount of remuneration owed to each advertiser.

This section of ISHIKAWA discloses that if a user identification code does not match known data, the entry is recorded in a spam system database 54. This section of ISHIKAWA does not disclose or suggest determining an occurrence of spamming on a web site based at least in part on identified normal users visiting the web site, as recited in claim 1. ISHIKAWA's determination of the occurrence of spam is in no way based at least in part on identified normal users visiting the web site, as recited in claim 1.

Since ISHIKAWA does not teach every aspect of the claimed invention recited in claim 1, ISHIKAWA cannot anticipate claim 1.

For at least the foregoing reasons, Applicants submit that claim 1 is not anticipated by ISHIKAWA.

Claims 2, 3, 6, 9-13, and 15 depend from claim 1. Therefore, these claims are not anticipated by ISHIKAWA for at least the reasons given above with respect to claim 1. Moreover, these claims recite additional features not disclosed or suggested by ISHIKAWA.

For example, claim 6 recites that tracking activities of users visiting a web site includes determining an interval at which each of the users visits the web site. The Examiner relies on paragraphs 0044, 0050, and 0055 of ISHIKAWA as allegedly disclosing this feature (Office Action, p. 4). Applicants respectfully disagree with the Examiner's interpretation of ISHIKAWA.

At paragraph 0044, ISHIKAWA discloses:

> The dynamically generated user identification code 34 can be any indicia which uniquely identifies the user and can be verified by the merchant. The identifying indicia generator 24 generates the user identification at the time that the advertisement or link is displayed, or loaded onto the user's

> computer 14, for instance, at the time that the advertisement or link is generated on a user's web page. In one preferred embodiment, the user identification comprises the user's IP address, wherein the IP address is derived via standard transmission protocols. In other embodiments, the user identification code 34 can be a time stamp, or any combination, including, but not limited to, a user IP address and a time stamp.

This section of ISHIKAWA discloses an identifying indicia generator 24 that generates user identification (which can be the user's IP address and/or a time stamp) at the time that an advertisement or link is displayed or loaded onto a user's computer 14. This section of ISHIKAWA does not disclose or suggest tracking activities of users visiting a web site that includes determining an interval at which each of the users visits the web site, as recited in claim 6. In fact, this section of ISHIKAWA does not even relate to tracking activities of users visiting a web site.

At paragraph 0050, ISHIKAWA discloses:

> If the user chooses to view the full advertisement or sales page, the user clicks onto the link and is transmitted to the merchant's web site. Upon the transfer of a user to the merchant's web site containing the advertisement, the identifying indicia, that is the confirmation code, is transmitted therewith 46. In addition, a second set of known user data is forwarded to the merchant. The second set of known user data is generated in accordance with standard transmission protocol and represents the most current user information. In one preferred embodiment, the known user data identifies the user's IP address, although any other type of data that can be used to identify the user, including, but not limited to, a time stamp, cookie, date and time stamp, or any combination thereof.

This section of ISHIKAWA discloses that when a user is transferred to a merchant's web site containing an advertisement, a second set of known user data is forwarded to the merchant, where the second set of known user data could include a time stamp, cookie, date and time stamp, or any combination thereof. ISHIKAWA does not disclose or suggest that this second set of known user data is used for tracking activities of users

visiting a web site as part of identifying normal users visiting the web site. Thus, this section of ISHIKAWA cannot disclose or suggest tracking activities of users visiting a web site that includes determining an interval at which each of the users visits the web site, as recited in claim 6.

At paragraph 0055, ISHIKAWA discloses:

> Similarly, if a time stamp is appended to the advertiser's identification, the merchant can then compare the actual time that the request is received at the merchant web site with the user's identification code, that is, the time stamp, as encrypted into the confirmation code. In this manner, the merchant can ascertain the length of time between the presentation of the advertisement link to the user and the response of the user, for example, the click by the user on the advertising link and the transmission of the request to the merchant's site. Thus, email transmissions of the advertisement would, in most instances, include a time stamp that reflects an unusual length of time between the presentation of the advertising link and the response to the advertisement.

This section of ISHIKAWA discloses a merchant comparing the actual time that the request is received at the merchant web site with the user's identification code, which includes a time stamp. ISHIKAWA does not disclose or suggest that the time stamp in the user's identification code is used for tracking activities of users visiting a web site as part of identifying normal users visiting the web site. Additionally, ISHIKAWA does not disclose that the time stamp is used for determining an interval at which each of the users visits the web site. Thus, this section of ISHIKAWA cannot disclose or suggest tracking activities of users visiting a web site that includes determining an interval at which each of the users visits the web site, as recited in claim 6.

Since ISHIKAWA does not teach every aspect of the claimed invention recited in claim 6, ISHIKAWA cannot anticipate claim 6.

For at least these additional reasons, Applicants submit that claim 6 is not anticipated by ISHIKAWA.

Claim 12 recites that the web site includes at least one advertisement. Claim 12 further recites that the determining an occurrence of spamming includes determining a click rate of the at least one advertisement for the identified normal users, and determining that the at least one advertisement has been spammed when the click rate of users visiting the web site exceeds the determined click rate for the identified normal users. ISHIKAWA does not disclose or suggest this combination of features.

For example, ISHIKAWA does not disclose or suggest determining a click rate of the at least one advertisement for the identified normal users. The Examiner relies on paragraphs 0010 and 0047 of ISHIKAWA as allegedly disclosing this feature (Office Action, p. 6). Applicants respectfully disagree with the Examiner's interpretation of ISHIKAWA.

At paragraph 0010, ISHIKAWA discloses:

> One method of increasing apparent clicks or viewing of an advertisement is to send the advertisement as an email. As each individual user retrieves their email, the advertisement containing the link, or the link alone, is displayed. If the user clicks on the advertisement or the link, some activity occurs to the advertisement site or sales page, such as, the user being transferred to the advertisement site or sales page. The clicking by the user on the advertisement or link causes the count of the clicks, that is, the number of responses, for the advertisement to be increased as the counter does not, and cannot, differentiate as to the manner in which the request to view the full advertisement is made, for example, through an email or on a web site page. As it is possible to send hundreds of thousands of emails at once, if all of the users who receive the advertisement or link in email, click on the advertisement or link, and, if clicking is the only criteria for payment, the fee due the advertiser can become an exorbitant amount. Although this may lead to some sales, it is problematic in that most of the audience of the advertising link is not a target audience. Thus, the

> merchant will, most likely, pay disproportionate advertising costs in relationship to the number of sales.

This section of ISHIKAWA discloses that clicking on an advertisement or link in an advertising email causes the count of the clicks for the advertisement to increase. This section of ISHIKAWA in no way relates to distinguishing normal and non-normal users. Thus, this section of ISHIKAWA cannot disclose or suggest determining a click rate of the at least one advertisement for the identified normal users, as recited in claim 12. In fact, this section of ISHIKAWA does not even relate to click rates.

At paragraph 0047, ISHIKAWA discloses:

> The plurality of databases 36 resides in the provider computer 12 or is coupled thereto on a storage medium 28. The plurality of databases 36 comprises a valid response database 38 and a invalid response database 40. The valid response database 38 represents fees owed to various advertisers for authentic or legitimate clicks, or genuine interest in the advertised data. In contrast, the invalid response database 40 represents clicks on advertisements that are deemed to be generated fraudulently. The advertiser's code 32 is recorded in this database in conjunction with the specific advertisement. In this manner, the merchant can monitor a particular advertiser to determine whether the advertiser is inappropriately marketing the product or service.

This section of ISHIKAWA discloses an invalid response database 40 that represents clicks on advertisements that are deemed to be generated fraudulently. This section of ISHIKAWA in no way discloses or suggests determining a click rate of the at least one advertisement for the identified normal users, as recited in claim 12. In fact, this section of ISHIKAWA does not even relate to click rates.

Since ISHIKAWA does not disclose or suggest determining a click rate of the at least one advertisement for the identified normal users, ISHIKAWA cannot disclose or suggest determining that the at least one advertisement has been spammed when the click

rate of users visiting the web site exceeds the determined click rate for the identified normal users, as also recited in claim 12. The Examiner relies on paragraphs 0012 and 0047 of ISHIKAWA as allegedly disclosing this feature (Office Action, p. 6). Applicants respectfully disagree with the Examiner's interpretation of ISHIKAWA.

At paragraph 0012, ISHIKAWA discloses:

> Currently, when a user clicks on an advertisement, or a link, some activity occurs, such as a transference of the user to the merchant's web page, where the full advertisement or sales page resides. In addition to the activity, for example, the transmission of the user to the web page, user information generated in accordance with standard transmission protocols and the advertiser's identification is also transmitted. The transmission of the advertiser's identification allows the merchant to identify which advertiser referred the user. In this manner, the merchant is able to count the number of clicks generated by a particular advertiser so that the advertiser can be appropriately paid for each advertisement. Indeed, merchants often utilize more than one source or advertiser, and thus, must be able to appropriately credit and assess which advertising modality is effective. As the merchant is currently only counting the number of clicks on the advertisement, if the clicks on the advertisement are the result of advertiser fraud, such as, "bulk emails", the merchant is unable to identify the click as resulting from a fraudulent advertising scheme and the advertiser is inappropriately paid. As stated above, in addition to the payment of fraudulent fees, the merchant can be subjected to legal action and loss of good will of the business. A need in the industry exists for a manner of authenticating responses to advertisements and the distribution modality of those advertisements. A further need exists for more accurately accessing the effectiveness of an advertising modality.

This section of ISHIKAWA discloses that a merchant is unable to identify advertising clicks that result from a fraudulent advertising scheme (such as bulk emails). This section of ISHIKAWA does not disclose or suggest determining that at least one advertisement has been spammed when the click rate of users visiting the web site exceeds the determined click rate for the identified normal users, as recited in claim 12. In fact, this section of ISHIKAWA does not even relate to click rates.

Paragraph 0047 of ISHIKAWA is reproduced above. This section of ISHIKAWA discloses an invalid response database 40 that represents clicks on advertisements that are deemed to be generated fraudulently. This section of ISHIKAWA in no way discloses or suggests determining that at least one advertisement has been spammed when the click rate of users visiting the web site exceeds the determined click rate for the identified normal users, as recited in claim 12. In fact, this section of ISHIKAWA does not even relate to click rates.

Since ISHIKAWA does not teach every aspect of the claimed invention recited in claim 12, ISHIKAWA cannot anticipate claim 12.

For at least these additional reasons, Applicants submit that claim 12 is not anticipated by ISHIKAWA.

Independent claims 16-18 recite features similar to (yet of different scope than) features described above with respect to claim 1. Therefore, Applicants submit that claims 16-18 are not anticipated by ISHIKAWA for at least the reasons given above with respect to claim 1.

Independent claims 19, 29, and 30 recite features similar to (yet possibly of different scope than) features described above with respect to claims 1 and 12. Therefore, Applicants submit that claims 19, 29, and 30 are not anticipated by ISHIKAWA for at least reasons similar to reasons given above with respect to claims 1 and 12.

Claims 20, 21, and 23-28 depend from claim 19. Therefore, these claims are not anticipated by ISHIKAWA for at least the reasons given above with respect to claim 19.

REJECTION UNDER 35 U.S.C. § 103(a) BASED ON ISHIKAWA AND WILLIAMS

Claims 4, 5, 7, 8, 14, 22, and 31 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over ISHIKAWA in view of WILLIAMS. Applicants respectfully traverse this rejection.

Claims 4, 5, 7, 8, and 14 depend from claim 1. The disclosure of WILLIAMS does not remedy the deficiencies in the disclosure of ISHIKAWA set forth above with respect to claim 1. Therefore, these claims are patentable over ISHIKAWA and WILLIAMS, whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 1.

Claim 22 depends from claim 19. The disclosure of WILLIAMS does not remedy the deficiencies in the disclosure of ISHIKAWA set forth above with respect to claim 19. Therefore, these claims are patentable over ISHIKAWA and WILLIAMS, whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 19.

Amended independent claim 31 is directed to a method for identifying normal users visiting a web site. The method includes tracking activities of users visiting the web site, where the tracking includes determining, for each user, at least one of whether the user loads images, an age of a cookie associated with each user, whether the user has javascript turned on, a type of browser used by the user, or an interval at which the user visits the web site; and identifying normal users based at least in part on the tracked activities. ISHIKAWA and WILLIAMS, whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, ISHIKAWA and WILLIAMS do not disclose or suggest identifying normal users based at least in part on tracking activities of users, where the tracking activities includes determining, for each user, at least one of whether the user loads images, an age of a cookie associated with each user, whether the user has javascript turned on, a type of browser used by the user, or an interval at which the user visits the web site. The Examiner relies on paragraphs 0015, 0016, and 0047 of ISHIKAWA for allegedly disclosing these features of claim 31 (Office Action, p. 19). Applicants respectfully disagree with the Examiner's interpretation of ISHIKAWA.

At paragraph 0015, ISHIKAWA discloses:

> When an advertising link is loaded onto a user's computer, a confirmation code is generated. If the user chooses to access the advertised materials, for example, the web page being advertised, the user clicks on the advertising link and is transmitted to the merchant's web site. As the user is transmitted to the merchant's web page, current user information generated in accordance with standard transmission protocols and the confirmation code are also transmitted.

This section of ISHIKAWA discloses that a confirmation code is generated when an advertising link is loaded onto a user's computer and transmitted to the merchant's web site when the user is transmitted to the merchant's web site. This section of ISHIKAWA does not disclose or suggest identifying normal users based at least in part on tracking activities of users, where the tracking activities includes determining, for each user, at least one of whether the user loads images, an age of a cookie associated with each user, whether the user has javascript turned on, a type of browser used by the user, or an interval at which the user visits the web site, as recited in claim 31. Receiving a

confirmation code from a user is not the same as identifying normal users based at least on part on tracking activities of users.

Paragraph 0016 of ISHIKAWA is reproduced above. This section of ISHIKAWA discloses comparing the dynamically generated user identification code to current user information to determine if a click is spam. This section of ISHIKAWA does not disclose or suggest identifying normal users based at least in part on tracking activities of users, where the tracking activities includes determining, for each user, at least one of whether the user loads images, an age of a cookie associated with each user, whether the user has javascript turned on, a type of browser used by the user, or an interval at which the user visits the web site, as recited in claim 31. At most, this section of ISHIKAWA can reasonably be said to disclose determining whether a particular click of an advertisement is spam based on a comparison of the current user information to the dynamically generated user identification code.

Paragraph 0047 of ISHIKAWA is reproduced above. This section of ISHIKAWA discloses an invalid response database 40 that represents clicks on advertisements that are deemed to be generated fraudulently. This section of ISHIKAWA does not disclose or suggest identifying normal users based at least in part on tracking activities of users, where the tracking activities includes determining, for each user, at least one of whether the user loads images, an age of a cookie associated with each user, whether the user has javascript turned on, a type of browser used by the user, or an interval at which the user visits the web site, as recited in claim 31. Storing information in a database representing clicks on advertisements that are deemed to be generated fraudulently is not equivalent to

identifying normal users based at least in part on tracking activities of users, where the tracking activities includes determining, for each user, at least one of whether the user loads images, an age of a cookie associated with each user, whether the user has javascript turned on, a type of browser used by the user, or an interval at which the user visits the web site, as recited in claim 31.

ISHIKAWA specifically discloses comparing current user identification information to user identification code generated dynamically at the time the advertising link is loaded onto the user's computer and storing an entry in a spam system database when the current user identification information does not match the user identification code (see, for example, paragraphs 0015 and 0016). ISHIKAWA in no way discloses or suggests identifying normal users based at least in part on tracking activities of users, where the tracking activities includes determining, for each user, at least one of whether the user loads images, an age of a cookie associated with each user, whether the user has javascript turned on, a type of browser used by the user, or an interval at which the user visits the web site, as recited in claim 31.

The disclosure of WILLIAMS does not remedy the above-identified deficiency in the disclosure of ISHIKAWA.

For at least the foregoing reasons, Applicants submit that claim 31 is patentable over ISHIKAWA and WILLIAMS, whether taken alone or in any reasonable combination.

In view of the foregoing amendments and remarks, Applicants respectfully request the Examiner's reconsideration of this application, and the timely allowance of the pending claims.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY SNYDER, L.L.P.

By: /John E. Harrity, Reg. No. 43367/
John E. Harrity
Registration No. 43,367

Date: August 6, 2007

11350 Random Hills Road
Suite 600
Fairfax, Virginia 22030
(571) 432-0800

Customer Number: 44989